Managing Information Security Breaches: Studies from Real Life

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University

Michael Krausz < http://linkedin.com/pub/michael-krausz/0/862/b55 > is a remarkable young man and a dynamic speaker. He visited Norwich University in November and gave a series of presentations there and at other institutions in Vermont on effective investigations of computer crimes.

Mr Krausz gave me a signed copy of his two books while he was in Vermont. *Managing Information Security Breaches* (ISBN 978-184928-094-5)< http://www.amazon.com/Managing-Information-Security-Breaches-Michael/dp/1849280940 > is a compact (183 pp) summary of fundamentals of incident response. The AMAZON link provides access to the table of contents.

I think that many readers will be particularly interested in Chapters 7, 8 and 9, which present case studies from small, medium, and large organizations respectively. Each case starts with an entertaining, well-written summary of the situation, continues to the "in-depth explanation" section and ends with lessons learned.

All of the cases are interesting, so I'm picking one pretty much at random. "A case of intrigue – the missing contract" starts with a merger of four companies who hired a managing director. For reasons unknown, the new managing director decided to attack one of the owners by finding information suitable for systematic defamation. The director was fired – and then, due to some legal complexities, fired again. In the period between the firings, the director signed a new contract for himself and for his assistant that awarded them significant new benefits. The two miscreants then threatened to sue their former employer based on these contracts. No one could find the contracts at first; the company laptops – reformatted before they were returned – had been assigned to new users and it took a forensic examination to locate the deleted contracts which, by chance, were on areas of the disk that had not been overwritten. Luckily, the former employees' claims were rejected in three courts.

The author points out that the lack of separation of duties (the "four-eyes" principle) allowed the new director to abuse the resources of his employer. Lack of precise planning for defining the duties of the new director allowed for abuse. There was no adequate termination agreement that could have limited recourse to the courts based on spurious contracts. All the employees had full access rights to their company laptops, allowing the miscreants to reformat their drives. There was no policy requiring anyone to create disk images from the company laptops before they were reassigned. The head of operations had limited knowledge of information technology (IT); his ignorance cause serious delays in locating the deleted information on disk.

Unfortunately, in this case, the company declined to change its culture of total trust, but at least they provided additional training for the employees managing their IT resources.

I very much enjoyed reading *Managing Information Security Breaches* and recommend it as the basis for good discussions in any organization. I am considering it for addition to my reading list in the “Management of Information Assurance”< http://www.mekabay.com/courses/academic/norwich/is342/index.htm > course I'll be teaching this year.

Krausz has also published a little pocketbook for reference. *Information Security Breaches: Avoidance and Treatment Based on ISO27001*< http://www.amazon.com/Information-Security-Breaches-Avoidance-Treatment/dp/1849280274 > is a 60-page booklet, perfect for sticking in a pocket, purse or briefcase, that can be used in meetings and discussions or just for thinking about.

Good work!

[Disclaimer: I have no financial involvement in Michael Krausz’s company or books; I just think he is a brilliant fellow who will continue to contribute to our field.]

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *